EXHIBIT 1

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JENNIFER L. MACPHERSON (202021)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SANTA CLARA – DOWNTOWN (DTS)

JOWELI VUNISA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

HEALTH NET, LLC, HEALTH NET OF CALIFORNIA, INC., HEALTH NET LIFE INSURANCE COMPANY, HEALTH NET COMMUNITY SOLUTIONS, INC., CALIFORNIA HEALTH & WELLNESS, CENTENE CORPORATION, and ACCELLION, INC., and DOES 1-50, inclusive,

Defendants.

Case No. **21CV379187**

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

BLOOD HURST & O'REARDON, LLP

Plaintiff JOWELI VUNISA ("Plaintiff"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through his attorneys, upon personal knowledge as to facts pertaining to himself and on information and belief as to all other matters, brings this class action against Defendants Health Net, LLC, Health Net of California, Inc., Health Net Life Insurance Company, Health Net Community Solutions, Inc., California Health & Wellness, Centene Corporation (collectively, "Health Net") and Accellion, Inc. (together, "Defendants"), and alleges the following:

NATURE OF THE CASE

1. Accellion, Inc. is a California-based private cloud solutions company that claims to provide secure third-party data file transfer services to over 3,000 customers worldwide. Accellion's File Transfer Appliance (FTA) software was developed 20 years ago as a secure way to overcome limits imposed on the size of email attachments. Health Net used Accellion's FTA services.

2. The FTA works like this: Users with access to the FTA log in through Accellion's portal and upload confidential information. Accellion's system then notifies the intended recipient that he/she has a secure file waiting. The recipient logs onto Accellion's system to retrieve the file.

3. Although the FTA is nearly 20 years old, it is still used by many organizations, including Health Net, in the finance, government and insurance sectors to transfer sensitive files. Accellion claims that for the last few years, it has encouraged its FTA customers to move to its new product, Kiteworks®, which it claims is more secure.

4. Transitioning away from FTA to a more secure software became critical last year when CentOS 6 - operating software that Accellion's FTA relies on to function - reached its end of life on November 30, 2020. Despite this end date, Accellion continued to support and some of its customers, like Health Net, continued to use the FTA to transfer sensitive personal and health information (PII/PHI).

5. In January 2021, Accellion disclosed that attackers breached its legacy FTA in mid-December with a SQL injection zero-day vulnerability. Accellion patched the SQL injection vulnerability and privately notified its customers, but the situation escalated as attackers

subsequently found more vulnerabilities and continued making attacks through January 2021 ("Data Breach").

6. Accellion claims about 100 of its FTA customers got hit and that of these about 25 lost a significant amount of data. The list of affected companies continues to grow and so far includes the Reserve Bank of New Zealand, the state of Washington, the Australian Securities and Investments Commission, the Singaporean telecom Singtel, the law firm Jones Day, the grocery store chain Kroger, the University of Colorado, the University of Maryland, Yeshiva University in New York, cybersecurity firm Qualys, Flagstar Bank, Canada's Bombardier, energy giant Shell, and Health Net.

7. Some of the exfiltrated data has ended up in the hands of the CLOP ransomware gang who is extorting affected companies. CLOP is exposing the data on a website it created on the dark web to pressure companies to pay money to remove their data from public view.

8. On March 25, 2021, Health Net reported the Data Breach to the California Attorney General. The sample notice of Data Breach is dated March 24, 2021 and confirms that member data was "view[ed] or download[ed]" by a malicious party in the Data Breach. It identifies the breached PII/PHI as including member names and one or more of the following: address, date of birth, insurance ID number and health information, such as patient medical condition(s) and treatment information.

9. Health Net's Data Breach notice omits critical facts such as the scope of member records that were breached and the time period of information breached (e.g., was it months or years of information).

10. In early March 2021, rather than notify affected members of the Data Breach, Health Net instead first sued Accellion in Chancery Delaware Court seeking indemnification for all costs and expenses arising out of the Data Breach, including the cost of notification, mitigation activities, and attorneys' fees. In its lawsuit, Health Net confirms hackers "downloaded" over 9GB of Health Net files and the Data Breach "exposed and compromised the PHI, PII and other confidential information of a significant number of Plaintiff's [Health Net's] members."

11. Defendants owed a duty to Plaintiff and Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the PII/PHI they collected and stored about them. Defendants breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect the PII/PHI from unauthorized access and unnecessarily using, storing and retaining Plaintiff's and Class members' personal information on Accellion's inadequately protected 20-year old legacy FTA software. Defendants knew that critical software necessary to operate the FTA, mainly CentOS 6, had an end life of November 30, 2020 at which point security updates would end. Despite knowing this, Defendants continued to use Accellion's FTA to store, maintain and transmit highly sensitive PII/PHI.

12. As a result of Defendants' inadequate cybersecurity, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings. Plaintiff brings this action on behalf of himself and all affected consumers in California whose PII/PHI was exposed as a result of the Data Breach.

13. Plaintiff seeks, for himself and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorneys' fees, litigation expenses and costs.

VENUE AND JURISDICTION

14. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class members pursuant to Cal. Code Civ. Proc. § 382.

15. This Court has personal jurisdiction over Defendants Accellion and Health Net because Defendants are headquartered in and have their principal place of business in California. This Court has personal jurisdiction over Defendant Centene Corporation because Centene conducts professional and commercial activities in California on a substantial, continuous, and systematic basis.

16. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendants regularly conduct business in this county, unlawful acts or omissions have occurred in this county, and Defendant Accellion is headquartered in this county.

THE PARTIES

17. Plaintiff Joweli Vunisa, is a citizen of California and resides in Sacramento, California. Plaintiff is insured through Health Net Community Solutions. As a member of Health Net, Plaintiff Vunisa, routinely provides Health Net with his confidential and highly sensitive PII/PHI when he seeks medical and/or dental treatment. On March 24, 2021, Health Net notified Plaintiff Vunisa that his PII/PHI was accessed by unauthorized users as a result of the Data Breach.

18. Defendant Accellion Inc. (Accellion) is a Delaware corporation with corporate headquarters located at 1804 Embarcadero Road, Suite 200, Palo Alto, California 94303. Accellion is a private cloud solutions company focused on secure file sharing and collaboration. Its products enable users to access, edit, and share enterprise content from any device.

19. Defendant Health Net, LLC ("HNL") is a Delaware limited liability company with dual headquarters in St. Louis, Missouri and Woodland Hills, California. HNL subsidiaries include Health Net of California, Inc., Health Net Life Insurance Company and Health Net Community Solutions, Inc. All are wholly owned subsidiaries of Centene Corporation. Through its operating subsidiaries, HNL delivers managed health care services through health plans and government-sponsored managed care plans. Health Net is a leading provider of health care coverage in California, with 3 million members statewide.

20. Defendant Health Net of California, Inc. (HNCA), is a California corporation, with dual headquarters in St. Louis, Missouri and Woodland Hills, California. HNCA is a California health care service plan licensed under the Knox-Keene Health Care Service Plan Act of 1975. It serves many counties throughout California.

21. Defendant Health Net Life Insurance Company (HNLI) is a California life and health insurance company with dual headquarters in St. Louis, Missouri and Woodland Hills, California. HNLI offers health insurance plans to residents of California.

22. Defendant Health Net Community Solutions, Inc. (HNCS) is a California corporation with dual headquarters in Woodland Hills, California and St. Louis Missouri. HNCS is a licensed health care service plan operating Medi-Cal and Medicare lines of business in California and is licensed under the Knox-Keene Health Care Service Plan Act of 1975.

23. Defendant California Health & Wellness (CHW) is a sister company of Health Net LLC and is a wholly owned subsidiary of Centene Corporation. CHW is a Medi-Cal plan that began serving Medi-Cal members in California in 2013 in California rural counties.

24. Defendant Centene Corporation is a Delaware corporation, with headquarters in St. Louis, Missouri. Centene is a multi-national healthcare enterprise that provides programs and services to government sponsored healthcare programs, focusing on under-insured and uninsured individuals. Centene operates in two segments, namely managed care and specialty services. In March 2016, Centene acquired Health Net.

25. Plaintiff is unaware of the true names and capacities of the Defendants sued herein as DOES 1 through 50, inclusive, and therefore sues these Defendants by such fictitious names pursuant to Cal. Civ. Proc. Code § 474. Plaintiff is informed and believes, and based thereon, alleges that each of the Defendants designated herein is legally responsible in some manner for the unlawful acts and occurrences complained of herein, whether such acts were committed intentionally, negligently, recklessly, or otherwise, and that each of the Defendants thereby proximately caused the injuries and damages to Plaintiff and the Class Members as herein alleged. Plaintiff will seek leave of Court to amend this complaint to reflect the true names and capacities of the Defendants when they have been ascertained and become known.

26. The agents, servants and/or employees of the Defendants and each of them acting on behalf of the Defendants acted within the course and scope of his, her or its authority as the agent, servant and/or employee of the Defendants, and personally participated in the conduct alleged herein on behalf of the Defendants with respect to the conduct alleged herein. Consequently, the acts of each Defendant are legally attributable to the other Defendants and all Defendants are jointly and severally liable to Plaintiff and other similarly situated employees, for the loss sustained as a proximate result of the conduct of the Defendants' agents, servants and/or employees.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right

27. PII/PHI is a valuable property right.[1] Indeed, the California Constitution guarantees every Californian the "inalienable right" to privacy. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[2]

28. The value of PII/PHI as a commodity is measurable.[3] "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market" for several years.

29. Companies recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

30. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be

---

[1] *See* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[2] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[3] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), *available at* http://www.medscape.com/viewarticle/824192.

[4] *See* Soma, *Corporate Privacy Trend, supra*.

[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/ assessment-tool.html.

aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

31. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[6] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen social security or credit card number.[7]

32. Recognizing the high value that consumers place on their PII/PHI, some companies offer consumers an opportunity to sell this information to advertisers and other third parties and California law imposes strict disclosure requirements when PII is shared or sold. Consumers are given more power over who ultimately receives their PII/PHI.

33. Consumers place a high value not only on their PII/PHI, but also on the *privacy* of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

---

[6] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), *available at* https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[7] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[8] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

34. Any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

35. Theft of PII/PHI is serious. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

36. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[10]

37. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[11] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receive bills; open new utilities; obtain a mobile phone; open a bank account

---

[9] *See* http:///www.gao.gov/new.items/d07737.pdf.

[10] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[11] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[12]

38. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[13] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[14] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[15]

39. A report published by the World Privacy Form and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.

---

[12] *See* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[13] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

[14] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

[15] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

40. A person whose PII/PHI has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

41. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[16]

42. It is within this context that Plaintiff and other Health Net Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for view and/or sale on the black-market.

Defendants' Businesses

43. Accellion, Inc. is a California-based private cloud solutions company founded in 1999 that focuses on products and services that enable companies to engage in secure file sharing and collaboration. Accellion claims to provide secure third-party data file transfer services to over 3,000 customers worldwide. Early demand for Accellion's file transfer applications came from organizations that needed to transfer large files. Accellion's FTA software met this demand by providing an email attachment application for reducing email storage and improving email performance by offloading file transfers from email. For over 20 years, companies used Accellion's FTA software to transfer large files.

44. Health Net provides health plans for individuals, families, businesses, and through Medicare and Medi-Cal. These health plans and services are offered through Health Net, LLC and its subsidiaries: Health Net of California, Inc., Health Net Life Insurance Company and Health Net

[16] *See* https://blog.linkedin.com/2016/05/18/protecting-our-members.

Community Solutions, Inc. These entities are wholly owned subsidiaries of Centene Corporation. Health Net has 3,000 employees and 85,000 network providers that serve more than 3 million members. Nearly 1 in 12 Californians are served by Health Net.

45. Upon information and belief Health Net's business operations are managed by a core group of individuals who oversee segments of business and thus the decision to use Accellion's FTA across the Health Net entities and to continue using it despite known vulnerabilities were centrally made by officers of Health Net LLC. For instance, Brian Ternan is the CEO of all the Health Net entities (except Centene). Martha Santana-Chin serves as the Government Programs Officer for Health Net in the California Market. She has executive oversight of Health Net's Medicare and Medi-Cal business lines and is responsible for positioning the business in the market and oversees the carrying out of Health Net's product and service area growths. Christy Bosse is the California Compliance Officer of Health Net, LLC. She leads the overall compliance program for the combined Health Net and California Health & Wellness health plan. Her responsibilities cover the CA market and all lines of business offered. And all of the Health Net entities are subsidiaries of Centene Corporation. As such, all Health Net Defendants played a role in the decision to continue to use outdated FTA software knowing it was vulnerable to attack and which resulted in the PII/PHI of its members being breached.

Health Net's Collection of Customers' PII/PHI

46. Health Net admittedly collects a substantial amount of PII and PHI from its members and prospective members. Health Net details the information it collects in its Notice of Privacy Practices (NPP),[17] Web Privacy Policy (WPP),[18] and its Privacy Notice for California Residents (California Privacy Notice).[19]

47. Health Net's NPP describes how it uses and discloses protected health information regarding its members. The NPP defines "PHI" as information about "you, including demographic

[17] https://www.healthnet.com/content/healthnet/en_us/disclaimers/legal/privacy-practices.html

[18] https://www.healthnet.com/content/healthnet/en_us/disclaimers/legal/privacy-policy.html

[19] https://www.healthnet.com/content/healthnet/en_us/disclaimers/legal/privacy-policy.html

information, that can reasonably be used to identify you and that relates to your past, present or future physical or mental health or condition, the provision of health care to you or the payment for that care."

48. Health Net's WPP explains how Health Net collects, uses, and discloses information about Health Net members or other individuals who visit its Website (www.healthnet.com). The WPP "applies to the collection, use and disclosure of information by Health Net, Inc. and its affiliated companies [] on www.healthnet.com and through mobile sites or social media [] as well as to information collected through telephone communications."

49. Incorporated into the WPP is Health Net's California Privacy Notice, "which supplements the information contained in California Health and Wellness (CHW) and Health Net, LLC's (and its subsidiaries, collectively 'Health Net') Privacy Policy, and applies solely to all visitors, users, and others who reside in the State of California." The notice is intended to comply with the California Consumer Privacy Act of 2018 (CCPA), and any terms defined in the CCPA have the same meaning as used in the California Privacy Notice.

Defendants' Promise to Safeguard Customer PII

50. The NPP promises that Health Net "protects your PHI." Health Net claims to protect member privacy in the following ways:

- We train our staff to follow our privacy and security processes.
- We require our business associates to follow privacy and security processes.
- We keep our offices secure.
- We talk about your PHI only for a business reason with people who need to know.
- We keep your PHI secure when we send it or store it electronically.
- We use technology to keep the wrong people from accessing your PHI.

51. The WPP promises that "Health Net takes reasonable steps to protect the security of your information, including use of appropriate physical, technical, and administrative safeguards." It advises that Health Net may disclose personal information to "unaffiliated companies such as agents or contractors ('Third Parties') [] to provide you with services that you have requested, or for other reasons related to the operation of our business" but promises that "in the event we provide

personal information to these Third Parties, they are restricted from using this data in any way other than to provide the required services for us."

52. The WPP also explains that "[y]our personal information and non-personal information may be stored in Health Net databases, affiliated company or subsidiary databases, or databases managed by third party service providers, which are located within and outside of the United States. Your information will be automatically transferred to these databases for storage and maintenance[.]"

53. Health Net's California Privacy Notice states that "Health Net may disclose your personal information to a third party for a business purpose" but promises that "[w]hen we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract." Health Net claims to share personal information with "Service providers" and "Data aggregators."

54. Accellion's business centers on helping companies securely transfer and utilize confidential and sensitive information. The "About Accellion" section portion of its website touts that "[t]he Accellion enterprise content firewall prevents data breaches and compliance violations from third party cyber risk. CIOs and CISOs rely on the Accellion platform for complete visibility, security and control over the communication of IP, PII, PHI, and other sensitive content across email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows. By consolidating security across third party communication channels, the Accellion content firewall simplifies complex infrastructure and reduces costs, while improving the user experience. When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[20]

55. Accellion also boasts that "[w]ith on-premise, private cloud, hybrid and FedRAMP deployment options, the Accellion content firewall provides the security and governance CISOs need to protect their organizations, mitigate risk, and adhere to rigorous compliance regulations such

[20] https://www.accellion.com/company/

as NIST 800-171, HIPAA, SOX, GDPR, CCPA, GLBA, and FISMA. Accellion solutions have protected more than 25 million end users at more than 3,000 global corporations and government agencies[.]"[21]

56. Accellion promises that its "file sharing and cloud services use industry-standard encryption usable in almost any regulatory situation. This includes integrated cloud services to share files in VDRs or through secure cloud and secure email sharing. These services offer services to support stringent compliance demands for file access and protection on top of useful features like automation and analytics."[22]

57. It also claims that using the FTA, "[f]iles are transferred through secure links and recipients are authenticated, which allows only the correct recipients to access the files."[23]

58. Despite these assurances and claims, Accellion failed to offer safe and secure file transfer products and services and failed to adequately protect Plaintiff's and Class members' PII/PHI entrusted to it by Accellion's clients, including Health Net.

The Data Breach

59. On January 12, 2021, Accellion publicly announced that it was made aware of a P0 vulnerability in its 20-year old legacy FTA software. Accellion claimed it had resolved the vulnerability and released a patch within 72 hours to the less than 50 customers affected.[24]

60. However, on February 1, 2021, Accellion acknowledged that hackers discovered and exploited additional vulnerabilities and the attack on its FTA software had continued into January 2021.[25] Joel York, Accellion's chief marketing officer, said after the first vulnerability was patched in December, the attackers came after the FTA again and again. "This was essentially cyber warfare between mid-December" and late January.[26]

---

[21] *Ibid.*

[22] https://www.accellion.com/secure-file-transfer/secure-file-share/

[23] https://www.networkcomputing.com/networking/accellion-no-file-too-big-new-file-transfer-appliance

[24] https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/

[25] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

[26] https://www.bankinfosecurity.com/blogs/accellion-mess-what-went-wrong-p-2989

61. Accellion's February 1 update titled "All Known Vulnerabilities Closed and Migration Efforts Continue" stated that "[i]n mid-December, Accellion was made aware of a zero-day vulnerability in its legacy FTA software. Accellion released a fix within 72 hours. This initial incident was the beginning of a concerted cyberattack on the Accellion FTA product that continued into January 2021. Accellion identified additional exploits in the ensuing weeks and rapidly developed and released patches to close each vulnerability. Accellion continues to work closely with FTA customers to mitigate the impact of the attack and to monitor for anomalies."

62. The February 1 release went on to state that "Accellion FTA, a 20 year old product nearing end-of life, was the target of a sophisticated cyberattack. All FTA customers were promptly notified of the attack on December 23, 2020." Accellion also claimed that it had "encouraged all FTA customers, which would include Health Net, to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible." Kiteworks® is Accellion's enterprise content firewall platform. The company describes it as a secure file sharing platform that facilitates access to enterprise content sources by allowing internal and external users to share, send, sync and edit files on any type of device from any content store.

63. On February 22, 2021, Accellion issued another update titled "Mandiant Identifies Criminal Threat Actor and Mode of Attacks[.]"[27] In it, Accellion explains that "Mandiant, a division of FireEye, Inc., has identified UNC2546 as the criminal hacker behind the cyberattacks and data theft involving Accellion's legacy File Transfer Appliance product. Multiple Accellion FTA customers who have been attacked by UNC2546 have received extortion emails threatening to publish stolen data on the "CL0P^_ - LEAKS" onion website. Some of the published victim data appears to have been stolen using the DEWMODE web shell. Mandiant is tracking the subsequent extortion activity under a separate threat cluster, UNC2582."

64. Accellion claimed it "does not access the information that its customers transmit via FTA. Following the attack, however, Accellion has worked at many customers' request to review

[27] https://www.accellion.com/company/press-releases/accellion-provides-update-to-fta-security-incident-following-mandiants-preliminary-findings/

their FTA logs to help understand whether and to what extent the customer might have been affected. As a result, Accellion has identified two distinct groups of affected FTA customers based on initial forensics. Out of approximately 300 total FTA clients, fewer than 100 were victims of the attack. Within this group, fewer than 25 appear to have suffered significant data theft."

65. On February 25, 2021, Accellion announced it was accelerating FTA's end-of-life to April 30, 2021 giving two reasons for this decision: (1) "The FTA software is Accellion's 20 year old legacy product. For the past three years, Accellion has been attempting to move its existing FTA customers over to our modern and more secure platform, Kiteworks®" and (2) "Six months ago, Accellion informed its FTA customers that the FTA operating system, CENTOS 6, had announced an end of life date of November 30, 2020. This limits our ability to support the FTA software."[28]

66. On March 1, 2021, Accellion posted another update titled "Mandiant validates full remediation of all known security vulnerabilities in the FTA product[.]"[29] This summarized the final report by FireEye Mandiant,[30] the cybersecurity forensics firm Accellion hired to conduct an investigation into the cyberattacks on its FTA software, and to review the FTA software for any other potential security vulnerabilities. This update stated that:

- **All known FTA vulnerabilities have been remediated:** Following penetration testing and code review, Mandiant has validated that Accellion has closed all known FTA vulnerabilities with patches issued soon after the vulnerabilities were identified.

- **Mandiant did not identify any additional vulnerabilities that were exploited by the attackers:** The previously remediated vulnerabilities were the only ones known to be involved in the December 2020 and January 2021 attacks. During their investigation, Mandiant identified two new vulnerabilities, which have since been patched, accessible only

[28] https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

[29] https://www.accellion.com/company/press-releases/accellion-provides-update-to-fta-security-incident-following-mandiants-preliminary-findings/

[30] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

by authenticated FTA users. Mandiant found no evidence that these vulnerabilities were exploited by threat actors.

67. Mandiant reported that attackers had reverse-engineered the nearly 20-year-old FTA code and found four zero-day flaws. Over the course of two separate attack campaigns in December and January, attackers exploited the flaws to drop a web shell onto any server running the FTA software, which they used to gain remote access and exfiltrate data.

68. The unknown attacker, which Mandiant calls UNC2546 exploited four zero-day vulnerabilities in the December and January attacks: CVE-2021- 27101, CVE-2021-27102, CVE-2021- 27103, and CVE-2021-27104.[31] CVE-2021-27101 is a SQL injection vulnerability that ranks a 9.8 on the National Institute of Standards and Technology's (NIST) Common Vulnerability Scoring System (CVSS). CVE-2021-27102 ranks a 7.8 and is an OS command injection vulnerability. The other two, CVE-2021-27103 and CVE-2021-27104, are a server-side request forgery bug and another OS command injection bug. Both rank a 9.8.[32]

69. The attackers exploited these vulnerabilities to install a Web shell named DEWMODE onto the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads are complete, the attackers then execute a clean-up routine to erase traces of their activity.[33]

PII/PHI Leaked on the Dark Web and Threat Actors Make Extortion Demands

70. The Data Breach was particularly damaging given the nature of Accellion's FTA. In the words of one industry expert: "[The] vulnerabilities [in Accellion's FTA] are particularly damaging, because in a normal case an attacker has to hunt to find your sensitive files, and it's a bit

---

[31] https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226

[32] https://www.databreachtoday.com/accellion-how-attackers-stole-data-ransomed-companies-a-16038

[33] https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226

of a guessing game, but in this case the work is already done . . . By definition everything sent through Accellion was pre-identified as sensitive by a user."[34]

71. Mandiant's final report published on March 1, states that the first SQL injection vulnerability was exploited by a group Mandiant calls UNC2546. UNC stands for uncategorized, which means that it cannot be linked yet to a known attack group. A few weeks later, some victims received ransom emails from a second group that claimed to be associated with the CLOP ransomware team, which Mandiant calls UNC2582. Mandiant notes there appears to be some overlap between CLOP, UNC2582 and another long-known group called FIN11, which has been around since at least 2016. FIN11 is known to specialize in phishing campaigns.[35]

72. Charles Carmakal, senior vice president and CTO at FireEye Mandiant comments that FIN11 maintained a high tempo of malicious activity through 2019 and 2020 but has been somewhat less so this year. "The threat group conducted widespread phishing campaigns targeting organizations in a broad range of sectors and geographic regions," he says. "We have not yet observed any FIN11 phishing campaigns in 2021—however, it is not unusual for the threat group to cease these operations for a month or two."[36]

73. UNC2582 threatened to publish data on the "CL0P^_- LEAKS" .onion shaming website, unless the victim paid an extortion fee. Mandiant reports that UNC2582 has followed through on threats to publish data, which has then shown up on the CLOP website.[37] As of March 30, 2021, there were 28 organization's on CLOP's website.[38]

74. According to Mandiant, UNC2582's pattern has been to steadily increase pressure on breached organization's—from initially sending emails to a small set of people from a single account to bombarding numerous recipients at the breached organization from hundreds of

---

[34] https://www.wired.com/story/accellion-breach-victims-extortion/

[35] https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

[36] https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226

[37] https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

[38] https://www.bankinfosecurity.com/blogs/accellion-holdouts-get-legacy-file-transfer-appliance-blues-p-3009

thousands of email addresses.[39] CLOP appears to be escalating its extortion tactics and has recently begun emailing customers of organizations for which it has stolen data, urging them to demand that the organization pay a ransom, or else it will begin dumping stolen information, including data pertaining to the email recipient.[40]

Health Net's Response to the Data Breach

75. On March 25, 2021, Health Net of California,[41] Health Net Life Insurance Company,[42] Health Net Community Solutions[43] and California Health & Wellness[44] reported the Data Breach to the California Attorney General.

76. Each notice explained that Health Net "used Accellion to exchange data files with health care providers and other vendors that support our operations." And that "[o]n January 25, 2021, Accellion informed us that its file transfer platform was compromised by an unknown malicious party. The compromise allowed the malicious party to view or download our data files stored on Accellion's system from January 7 to January 25, 2021."

77. Health Net identified the PII/PHI involved in the Data Breach as including member names and one or more of the following: address, date of birth, insurance ID number and health information, such as patient medical condition(s) and treatment information.

78. Health Net claimed that upon learning of the incident it activated its "incident response plan and worked with Accellion to conduct" its own investigation to analyze the files involved so it "could distribute notification to affected individuals as quickly as possible." Health Net also "stopped using Accellion's services and removed all of [Health Net's] data files from

---

[39] https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

[40] https://www.bankinfosecurity.com/blogs/accellion-holdouts-get-legacy-file-transfer-appliance-blues-p-3009

[41] https://oag.ca.gov/system/files/Health%20Net%20of%20California%20-%20Accellion%20Breach%20Notice%20Letter.pdf

[42] https://oag.ca.gov/system/files/Health%20Net%20Life%20Insurance%20Company%20-%20Accellion%20Breach%20Notice%20Letter.pdf

[43] https://oag.ca.gov/system/files/Health%20Net%20Community%20Solutions%20-%20Accellion%20Breach%20Notice%20Letter.pdf

[44] https://oag.ca.gov/system/files/California%20Health%20%26%20Wellness%20-%20Accellion%20Breach%20Notice%20Letter.pdf

[Accellion's] system" and "reviewed our other file transfer service processes and tools to ensure they are not at risk of a similar attack."

79. Health Net's notice of Data Breach fails to provide adequate remediation. Health Net's offer of one year of free identity protection is insufficient given the high value placed on PHI (particularly when combined with PII) by identity thieves and the fact that individuals whose PHI was breached are vulnerable to attack for years to come. Medical identity theft may take twice as long to discover and the impact can have severe consequences. For instance, thieves may use stolen PHI to see a doctor, get prescription drugs, file claims. And if the thief's health information is mixed with the victim's this can have devastating consequences to a victim's health.

80. Health Net's notice of the Data Breach also fails to provide sufficient detail about what PII/PHI was accessed and by whom. Health Net states only that health information, such as patient medical condition(s) and treatment information was breached but fails to provide any specifics including the time period of the information breached. For instance, was it only patient data for the last year or did it go back years?

81. Health Net also fails to warn members that some data involved in the Data Breach (albeit from other companies) has been leaked on the dark web and is being used as a means to extort ransoms from companies involved in the Data Breach and that these bad actors have gone so far as to email customers whose PII/PHI was stolen (the true victims). Health Net fails to say whether it has been subject to any ransom demand.

82. Health Net's failure to provide a detailed description of what PII/PHI was accessed and by whom has left Plaintiff and Class members in the dark. By failing to adequately inform Plaintiff and Class members of the exact information that was breached and the above-mentioned details surrounding the Data Breach Plaintiff and Class members are unable to adequately protect themselves against medical and identity theft.

83. While Health Net waited until March 24, 2021 to notify affected members it filed a lawsuit on March 10, 2021, against Accellion for breach of contract and declaratory relief in Delaware Chancery Court seeking among other things indemnification from Accellion for all costs

and expenses arising out of the Data Breach, including the cost of notification, mitigation activities, and attorneys' fees.

84. Health Net's lawsuit reveals critical facts it omits from its Data Breach notice to members. In it, Health Net admits Accellion notified it on December 21, 2020 that certain FTA vulnerabilities had been exploited but claims Accellion failed to mention any customer data had been stolen. Health Net alleges its customer data was not breached until January 20, 2021, when hackers exploited another vulnerability in the FTA software.

85. According to Health Net's complaint, hackers obtained Accellion's encryption keys, which allowed them to decrypt files they took from Accellion. Hackers then "downloaded" over 9GB of Health Net files. The Data Breach "exposed and compromised the PHI, PII and other confidential information of a significant number of Plaintiff's [Health Net's] members."

86. Health Net also admits that it used Accellion's FTA to transfer patient PII and PHI with providers. The FTA is a cloud-based, file transfer service offered by Accellion that is used to "transfer large and sensitive files securely." Health Net explained how the FTA worked in the following way: a Health Net employee with access to the FTA will log in through Accellion's portal and upload confidential information. Accellion's system will send a notification to the intended recipient that he/she has a secure file waiting. The recipient will log onto Accellion's system and retrieve the file. Accellion's system maintains and stores transferred PII/PHI for up to 30 days.

87. Although Health Net knew the FTA was exploited as early as December 21, 2020 it waited over three months to notify members. Further, it failed to inform members about the scope of the Data Breach specifically that over 9GB of Health Net files were breached affecting a "significant number" of its members.

Health Net's Notice of Data Breach

88. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters must be sent to residents of California "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]"

89. Health Net's sample Data Breach letters were filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f).

90. Plaintiff's and Class members' PII/PHI is "personal information" as defined by California Civ. Code § 1798.82(h).

91. California Civ. Code § 1798.82(g) defines "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

92. The Data Breach was a "breach of the security of the system" as defined by California Civ. Code § 1798.82(g).

93. Thus, Health Net filed and disseminated its breach notification because Plaintiff's and Class members' unencrypted personal information was acquired by an unauthorized person or persons as a result of the Data Breach.

94. On March 25, 2021, Defendants Health Net of California, Health Net Life Insurance Company, Health Net Community Solutions and California Health & Wellness filed a notice with the U.S. Department of Health and Human Services Office for Civil Rights indicating a "Hacking/IT Incident" of unsecured protected health information of tens of thousands of individuals. Health Net of California reported that the breach affected 523,709 individuals, Health Net Life Insurance Company reported that the breach affected 16,637 individuals, Health Net Community Solutions reported that the breach affected 686,556 individuals and California Health & Wellness reported that the breach affected 80,138 individuals.

95. The breach report filed by Health Net entities on March 25, 2021, with the Secretary of the U.S. Department of Health and Human Services was filed in accordance with 45 CFR § 164.408(a).

96. Pursuant to 45 CFR § 164.408(a), breach reports are filed with the Secretary of the U.S. Department of Health and Human Services "following the discovery of a breach of unsecured protected health information."

97. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

98. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

Defendants Knew the FTA Was Vulnerable to Attack

99. Accellion's FTA product, which Health Net and certain of its other clients used, was not secure and, by Accellion's own acknowledgment, outdated.

100. Accellion acknowledged that the FTA program is insufficient to keep file transfer processes secure "in today's breach-filled, over-regulated world" where "you need even broad protection and control."[45] On the page dedicated to Accellion FTA, Accellion's website states: "End-of-Life Announced for FTA. No Renewals After April 30, 2021."[46]

101. Key people within Accellion have acknowledged the need to leave the FTA platform behind due to the security concerns raised by it. Accellion's Chief Marketing Officer Joel York confirmed that Accellion is encouraging its clients to discontinue use of FTA because it does not protect against modern data breaches: "It just wasn't designed for these types of threats . . . ."[47]

102. Accellion's Chief Information Security Officer Frank Balonis stated: "Future exploits of [FTA] . . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[48]

---

[45] https://www.accellion.com/products/fta/

[46] *Id.*

[47] https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/

[48] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

103. Despite knowing that FTA left Accellion's customers (like Health Net) and third parties interacting and transacting with its customers (like Plaintiff and Class Members) exposed to security threats, Accellion continued to offer and Health Net continued to utilize the FTA file transfer product at the time of the Data Breach.

104. On information and belief, Health Net failed to make the switch to Kiteworks® and knowingly continued to use FTA, exposing its members' PII/PHI to the risk of theft, identity theft, and fraud.

105. On February 25, 2021, Accellion formally announced that it was accelerating FTA's end-of-life to April 30, 2021. Accellion claims that for the last three years it has been urging existing FTA customers to migrate to what it describes as Accellion's more secure platform, Kiteworks®.[49] As an incentive, Accellion offered a license and free migration support to Kiteworks®.[50]

106. Accellion also states that as early as August 2020, it was informing FTA customers that the FTA operating system, CentOS 6, had announced an end of life date of November 30, 2020 and that this would limit Accellion's ability to support the FTA software.[51]

107. End of Life means a product is no longer supported. As such, CentOS would no longer provide security updates or fix bugs. Thus, it was important for companies to upgrade or migrate to newer versions of CentOS before they become end of life.[52]

108. Indeed, in late 2019, CentOS announced that it was no longer supporting CentOS 6 after November 30, 2020.[53] CentOS is a Linux distribution that provides a free, enterprise-class, community-supported computing platform functionally compatible with its upstream source, Red

---

[49] https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

[50] https://www.databreachtoday.com/blogs/accellion-mess-what-went-wrong-p-2989 (Feb. 3, 2021)

[51] https://www.accellion.com/company/security-updates/accellion-announces-end-of-life-eol-for-its-legacy-fta-product/

[52] https://www.hostdime.com/blog/centos-6-end-of-life/

[53] https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/; https://wiki.centos.org/FAQ/General#What_is_the_support_.27.27end_of_life.27.27_for_each_CentOS_release.3F; https://endoflife.date/centos; https://support.cpanel.net/hc/en-us/articles/360058490254--CentOS-6-End-of-Life-Notice; https://wiki.centos.org/About/Product

Hat Enterprise Linux. CentOS 6 was released on July 10, 2011, active support ended on May 10, 2017, and its end-of-life was planned for and occurred on November 30, 2020.[54]

109. Accellion's FTA relies on CentOS 6 to function and the company claims that it planned to migrate all its FTA customers to Kiteworks® before the November 30 cut-off date but failed.[55] York, Accellion's chief marketing officer, speculated that customers may have been dissuaded from converting because of the time and cost involved. For instance, "[d]ata has to be migrated, processes need to be changed and employees need to be trained on the new system."[56] Accellion fails to explain, however, why if it knew in 2019 that CentOS 6 was going to reach its end of life it did not start notifying customers until August 2020, just months before.

110. Karen Walsh, CEO at Allegro Solutions, told TechRepublic that the Accellion "breach is another example of cybercriminals looking to exploit end-of-life tools, increasing the amount of scrutiny that companies should be placing on their legacy technologies. Functionally, this is an example of how supply chains create a domino effect[.]" And "[u]ltimately, this means that Accellion FTA customers were running a service that relied on a now-unsupported technology. As CentOS moved to end-of-life, Accellion needed to move their customers to a new platform. In the meantime, these malicious actors used a traditional SQL injection methodology to gain access."[57]

111. Oliver Tavakoli, CTO at Vectra, also commented to TechRepublic that the attack should serve as a reminder that security teams need to be keenly aware of the third-party tools they use, particularly with sensitive data, and to aggressively patch them. Tavakoli also noted that organizations had to do a closer analysis of any legacy/near-end-of-life products which may no onger be receiving the expected vulnerability testing efforts.

112. Chloé Messdaghi, chief strategist at Point3 Security, notes that many organizations in the financial, government and commercial sectors still use FTA to transfer large files, despite

---

[54] https://endoflife.date/centos

[55] https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/

[56] https://www.bankinfosecurity.com/blogs/accellion-mess-what-went-wrong-p-2989)

[57] https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/

Accellion's offering of newer and more secure file-sharing solutions. "That's problematic – it's the kind of decision that puts companies at sharply increased risk[.]" "The fact is that breaches are going to happen and possibly through a third party. The takeaway is that when a company pushes out security updates and urges their customers to adopt them, companies then need to take that advice and implement them. Like patches, product upgrades are crucial to sustaining a strong security posture."[58]

113. Health Net fails to indicate the time period of member PII/PHI involved in the Data Breach. Was it information Health Net sent in the last 30 days or was it information from months or even years before that Health Net had not (or had nor confirmed had been) purged from the FTP? This is critical. David Stubley, a response expert who heads Edinburgh, Scotland-based security testing firm and consultancy 7 Elements warns that the "[k]ey for all services and products is to ensure file upload/sharing permissions are set correctly and reviewed regularly, client files are purged when no longer needed or moved to longer-term encrypted storage, and software updated on a continuous basis." He also explains that "[t]he key is to treat the individual file with the appropriate level of protection. If the file contains sensitive information, it should be encrypted at rest, transferred in an encrypted state and if possible, removed once successfully delivered."[59]

Defendants Knew or Should Have Known PII/PHI Are High Risk Targets

114. Defendants knew or should have known that PII, and in particular, PHI, are high risk targets for identity thieves. In 2014, the FBI informed that "[c]yber actors will likely increase cyber intrusions against healthcare systems" and warned that the "healthcare industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures[.]"[60]

115. The Identity Theft Resource Center reported that the Medical/Healthcare sector had the second largest number of breaches in 2018 and the highest rate of exposure per breach.

---

[58] https://www.bankinfosecurity.com/singtel-qimr-berghofer-hit-by-accellion-vulnerability-a-15982

[59] https://www.bankinfosecurity.com/blogs/accellion-holdouts-get-legacy-file-transfer-appliance-blues-p-3009

[60] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/

According to the ITRC this sector suffered 363 data breaches exposing over 9 million records in 2018.[61] These included Blue Cross Blue Shield of Michigan (15K records exposed), Atrium Health (over 2M records exposed), UnityPoint Health (over 1M records), LifeBridge Health (over 500K), FastHealth Corporation (over 600K records), among others.

116. Both Health Net and Centene knew they were at risk of a data breach and that customer PII/PHI was vulnerable and in demand. In a letter dated January 29, 2016, ConsumersUnion responded to the planned merger of Centene and Health Net by urging "the [California] Department [of Insurance] to closely scrutinize this deal" for a number of reasons including "data security."[62] ConsumersUnion commented that while "Health Net acknowledged a prior security lapse, which was the subject of a penalty by DMHC, and detailed its efforts to improve [] Centene was less forthcoming; it failed to acknowledge that the plan is actually currently missing six hard drives containing the personal and health information of nearly 950,000 individuals. This significant omission to the department suggests a lack of appreciation for either the gravity of the situation or the importance of transparency with regulators, policyholders, and the general public." ConsumersUnion warned that if the "merger is approved, Centene and Health Net will be tasked with combining two large data systems into one, perhaps leaving policyholders even more vulnerable to security lapses[.]"

117. As such, Defendants were aware that PII/PHI is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII/PHI against cyber-security attacks that Defendants should have anticipated and guarded against.

CLASS DEFINITION AND ALLEGATIONS

118. Pursuant to Cal. Code Civ. Proc. § 382, Plaintiff seeks certification of a class defined as: All California residents whose PII/PHI was subjected to the Data Breach.

---

[61] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[62] http://www.insurance.ca.gov/0250-insurers/0500-legal info/upload/FinalExhibitBinderHealthNetCenteneHearingPart-1.pdf (p. 362)

119. Excluded from the Class are: (1) Defendants and their officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

120. While the exact number of Class members is unknown, Health Net acknowledges the Data Breach involved over 9GB of Health Net files and the Data Breach "exposed and compromised the PHI, PII and other confidential information of a significant number of Plaintiff's [Health Net's] members." Health Net's notice to the HHS indicates that over one million individuals were affected by the Data Breach. Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

121. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

122. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI it collected from Plaintiff and Class members;

(b) Whether Defendants breached their duties to protect the PII/PHI of Plaintiff and each Class member; and

(c) Whether Plaintiff and each Class member are entitled to statutory damages, actual damages, and other equitable relief.

123. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to or that

conflict with the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

124. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class may be relatively small. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

125. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive and declaratory relief with respect to the Class as a whole.

FIRST CAUSE OF ACTION

Violation of the California Confidentiality of Medical Information Act

(Civil Code §§ 56, *et seq.*)

(Plaintiff and Class Against All Defendants)

126. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

127. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

128. Civ. Code § 56.10(d) says "[e]xcept to the extent expressly authorized by a patient, enrollee, or subscriber, or as provided by subdivisions (b) and (c), a provider of health care, health care service plan, contractor, or corporation and its subsidiaries and affiliates shall not intentionally

share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient." Civ. Code § 56.10(e) contains a similar prohibition that "a contractor or corporation and its subsidiaries and affiliates shall not further disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan or insurer or self-insured employer received under this section to a person or entity that is not engaged in providing direct health care services to the patient."

129. Health Net of California and Health Net Community Services are a "provider of health care" and/or "service plan" within the meaning of Civil Code § 56.06 and are entities regulated pursuant to the Knox-Keene Health Care Service Plan Act of 1975, and are therefore subject to the requirements of the CMIA. Defendants Health Net, LLC, California Health & Wellness, and Centene Corporation are subsidiaries and/or affiliates of Health Net of California and Health Net Community Services pursuant to Civil Code § 56.10(d) and thus are subject to the CMIA. Accellion is a "contractor" within the meaning of Civil Code § 56.05 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Health Net and Centene, within the meaning of Civil Code § 56.05(k).

130. Plaintiff and all members of the Class are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and the Class fear that disclosure of their medical information could subject them to harassment or abuse.

131. Plaintiff and the respective Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, stored, abandoned, destroyed or disposed of on and/or via Defendants' computer networks at the time of the Data Breach.

132. Defendants, through inadequate security, allowed an unauthorized third party to gain access to, view and/or download Plaintiff's and each Class members' medical information, without

the prior written authorization of Plaintiff and the Class members, as required by Civil Code § 56.10 of the CMIA.

133. In violation of Civil Code § 56.10(a), Health Net Defendants disclosed Plaintiff's and Class members' medical information without first obtaining an authorization. Plaintiff's and Class members' medical information was actually viewed by unauthorized individuals as a direct and proximate result of Health Net Defendant's violation of Civil Code § 56.10(a). Health Net's notice of data breach to Plaintiff Vunisa confirmed his PII/PHI was viewed stating "[t]he compromise allowed the malicious party to view or download our files stored on Accellion's system from January 7 to January 25, 2021" and confirmed that it had determined that Plaintiff's "personal information was included in the data files involved in this incident."

134. Health Net Defendants disclosed medical information pertaining to members of the proposed Class to unauthorized persons without first obtaining consent, in violation of Civil Code §56.10(a). Health Net continued to use and actively uploaded and transferred sensitive files using Accellion's legacy FTA software despite knowing the software lacked adequate security to protect its members' PII/PHI particularly because its supporting software CentOS 6 had reached its end of life. In addition, upon information and belief, Health Net failed to timely remove member files from the FTA in order to further safeguard this information in the event of a data breach. By uploading and transferring files using the FTA and failing to timely remove member files from the FTA, Health Net took affirmative actions that resulted in the disclosure of information to and its viewing by unauthorized individuals in the Data Breach in violation of Civil Code § 56.10(a).

135. In violation of Civil Code § 56.10(e), Defendant Accellion further disclosed Plaintiff's and Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or Class members or their providers of health care or health care service plans or insurers or self-insured employers. Accellion's affirmative actions include, among other things, failing to transition its clients from the legacy FTA software, which it knew lacked adequate security to protect Plaintiff's and Class members' PII/PHI, prior to the end of life date of its supporting CentOS 6 software. This resulted in the Data Breach, by which Accellion

disclosed medical information pertaining to Plaintiff and members of the proposed Class to unauthorized persons without first obtaining consent, in violation of Civil Code § 56.10(e).

136. Defendants violated Civil Code § 56.101 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

137. In violation of Civil Code § 56.101(a), Defendants created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiff's and Class members' medical information was actually viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(a).

138. In violation of Civil Code § 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class members' medical information. Plaintiff's and Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(a). Health Net's notice of data breach to Plaintiff Vunisa confirmed the information was viewed stating "[t]he compromise allowed the malicious party to view or download our files stored on Accellion's system from January 7 to January 25, 2021."

139. Plaintiff's and Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

140. In violation of Civil Code § 56.101(b)(1)(A), Defendants' electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff's and Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(b)(1)(A).

141. Defendants violated Civil Code § 56.36 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

142. As a result of Defendants' above-described conduct, Plaintiff and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

143. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

144. Plaintiff, individually and for each member of the Class, seeks statutory damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), actual damages suffered pursuant to Civil Code § 56.36(b)(2), injunctive relief, and punitive damages of up to $3,000 per Plaintiff and each Class member, attorneys' fees, litigation expenses and court costs pursuant to Civil Code § 56.35.

SECOND CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 (CCPA)

Cal. Civ. Code §§ 1798.100, *et seq.*

(Plaintiff and Class Against All Defendants)

145. Plaintiff realleges and incorporate by reference all proceeding paragraphs as if fully set forth herein.

146. To the extent the Data Breach of Health Net members includes information that is not "protected health information" as that term is used in Cal. Civ. Code § 1798.145(c), Plaintiff brings this claim for breach of PII and/or "patient information" that does not constitute PHI. Entities

covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must still protect personal data that is covered by the CCPA but does not satisfy the definition of PHI under HIPAA. Health Net's vague and inadequate Data Breach letters fail to describe the specific information that was breached much of which may be PII that is not PHI or "patient information" and thus covered by the CCPA.

147. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[63]

148. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendants failed to implement such procedures which resulted in the Data Breach.

149. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

[63] CCPA, Section 2(f).

150. Plaintiff Vunisa is a "consumer" as defined by Civ. Code § 1798.140(g) because he is "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

151. Defendants are a "business" as defined by Civ. Code § 1798.140(c) because Defendants:

a. are a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in and is headquartered in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

152. Plaintiff Vunisa's PII was subject to unauthorized access and exfiltration, theft or disclosure because his PII, including name, address, date of birth, insurance ID number and health information such as medical condition(s) and treatment information, was subject to unauthorized access and exfiltration, theft, or disclosure.

153. Plaintiff's PII was in nonencrypted and nonredacted form, allowing criminals full access to it.

154. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Defendants failed to implement reasonable security procedures to prevent

unauthorized access of Plaintiff Vunisa's and Class members' PII as a result of the attack identified by FireEye Mandiant.

155. Attached as Exhibit A is written notice Plaintiff provided to Defendants pursuant to Civil Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have or are violating. Although a cure is not possible under the circumstances, if as expected Defendants are unable to cure or do not cure the violation within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

156. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

THIRD CAUSE OF ACTION

Violation of the California Unfair Competition Law

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

(Plaintiff and Class Against All Defendants)

157. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

158. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

159. In the course of conducting their business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII/PHI, and by violating the statutory and common law alleged herein, including, *inter alia*, California's Confidentiality of Medical Information Act (Civ. Code §§ 56.10(a), (e);

56.101(a), 56.101(b)(1)(A); 56.36), California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.150(a)(1)), and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiff and Class members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

160. Health Net also violated the UCL's unlawful prong by breaching contractual obligations created by its Privacy Policies and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of its posted privacy policy. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Health Net's violations of its Privacy Policies.

161. Defendants violated the UCL by failing to adequately and timely notify Plaintiff and Class members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class members had been adequately and timely notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

162. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII/PHI and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, CMIA, Article I, Section 1 of the California Constitution (California's constitutional right to privacy), and the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45). The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

163. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Health Net's violations of its Privacy Policies and statutory and common law in that a portion of the money Plaintiff and Class members paid for Health Net's products and services went to fulfill the contractual obligations set forth in Health Net's Privacy Policies, including maintaining the security of their PHI, and Health Net's legal obligations and Health Net failed to fulfill those obligations.

164. The UCL also prohibits any "fraudulent business act or practice." Defendants' above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

165. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendants' unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PHI but receiving a lower level, paying more for Health Net's products and services than they otherwise would have had they known Defendants were not providing the reasonable security represented in Health Net's Privacy Policies and in conformance with their legal obligations. Had Plaintiff and Class members known about Defendants' substandard data security practices they would not have purchased Health Net's products or services or would have paid less for them. Defendants' security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII/PHI.

166. Plaintiff and Class members have also suffered (and will continue to suffer) loss of money and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity and medical theft and identity and medical fraud which require paying for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the CMIA and CCPA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

167. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, Class members, and the general public, also seek restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

FOURTH CAUSE OF ACTION

SEVENTH CAUSE OF ACTION

Invasion of Privacy

(Plaintiff and Class Against All Defendants)

168. Plaintiff realleges and incorporate by reference all proceeding paragraphs as if fully set forth herein.

169. Plaintiff and Class members have a legally protected privacy interest in their PII/PHI that Defendants required them to provide and allow it to store.

170. Plaintiff and Class members reasonably expected their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

171. Defendants unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

172. In failing to adequately secure Plaintiff's and Class members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their

substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

173. Defendants violated Plaintiff's and Class members' right to privacy under the common law as well as under state and federal law.

174. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class/ members have suffered injury as a result of Defendant's unlawful invasions of privacy and are entitled to appropriate relief.

EIGHTH CAUSE OF ACTION

Breach of Contract

(Plaintiff and Class Against Defendants Health Net and Centene)

175. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

176. Health Net's Privacy Policies – the NPP, WPP, California Privacy Notice - formed an express contract in which Defendants promised to protect nonpublic personal information given to Defendants or that Defendants gathered on their own, from disclosure.

177. Plaintiff and Class members performed their obligations under the contracts when they provided their PII/PHI to Defendants in relation to their purchase of Defendants' products and services.

178. Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was exposed as part of the Data Breach.

179. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

NINTH CAUSE OF ACTION

Breach of Implied Contract

(Plaintiff and Class Against Defendants Health Net and Centene)

180. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

181. Defendants provided Plaintiff and Class members with an implied contract to protect and keep their PII/PHI private.

182. Plaintiff and Class members would not have provided their PII/PHI to Defendants or its subsidiaries or contractors, but for Defendants' implied promises to safeguard and protect their information.

183. Plaintiff and Class members performed their obligations under the implied contract when they provided their PII/PHI to Defendants to obtain and use their products and services.

184. Defendants breached the implied contract with Plaintiff and Class members by failing to protect and keep private their PII/PHI.

185. As a direct and proximate result of Defendants' breach of their implied contract, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

TENTH CAUSE OF ACTION

ELEVENTH CAUSE OF ACTION

Declaratory Relief

(Plaintiff and Class Against All Defendants)

186. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

187. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' duties to safeguard and protect Plaintiff's and Class members' PII/PHI. Defendants' PII/PHI security measures were (and continue to be) woefully inadequate. Defendants likely dispute these contentions and contends their security measures are appropriate.

188. Plaintiff and Class members continue to suffer damages, other injury or harm as additional identity and financial theft and fraud occurs.

189. Therefore, Plaintiff and Class members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, *inter alia*, (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiff's and Class members' confidential and sensitive personal information, and timely notify them about the Data Breach, (ii) Defendants breached (and continue to breach) such legal duties by failing to safeguard and protect Plaintiff's and Class members' PII/PHI, and (iii) Defendants' breach of their legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiff and Class members. A declaration from the Court ordering Defendants to stop their illegal practices is required. Plaintiff and Class members will otherwise continue to suffer harm as alleged above.

PRAYER FOR RELIEF

190. **Damages.** As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members suffered (and will continue to suffer) actual and statutory damages and other injury and harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, CCPA and the UCL, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages. Plaintiff and Class members also are entitled to equitable relief, including, without limitation, restitution. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

191. **Punitive Damages.** Plaintiff and Class members also are entitled to punitive damages from Defendants, as punishment and to deter such wrongful conduct in the future, pursuant

to, *inter alia*, California common law. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

192. **Injunctive Relief.** Pursuant to, *inter alia*, the California UCL, Plaintiff and Class members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) Internet monitoring, (iii) identity theft insurance, (iv) prohibiting Defendants from continuing its above-described wrongful conduct, (v) requiring Defendants to modify their corporate culture and implement and maintain reasonable security procedures and practices to safeguard and protect the PII/PHI entrusted to them, (vi) periodic compliance audits by a third party to ensure that Defendants are properly safeguarding and protecting the PII/PHI in their possession, custody and control, and (vii) clear and effective notice to Class members about the serious risks posed by the exposure of the personal information and the precise steps that must be taken to protect themselves. All conditions precedent to Plaintiff's and Class members' claims for relief have been performed and occurred.

193. **Attorneys' Fees, Litigation Expenses and Costs.** Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action.

WHEREFORE, Plaintiff, on behalf of himself and all members of the Class respectfully request that (i) this action be certified as a class action, (ii) Plaintiff Joweli Vunisa be designated representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class. Plaintiff, on behalf of himself and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendants for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) statutory damages (except as to the CCPA at this time);

(iii) equitable relief, including restitution;

(iv) pre- and post-judgment interest at the highest legal rates applicable;

(v) appropriate injunctive relief;

(vi) attorneys' fees and litigation expenses;

(vii) costs of suit; and

(viii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable

Respectfully submitted,

Dated: April 6, 2021

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JENNIFER L. MACPHERSON (202021)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff

Exhibit A

BLOOD HURST & O'REARDON | LLP

501 W. Broadway, Suite 1490 | San Diego, CA 92101
T | 619.338.1100 F | 619.338.1101
www.bholaw.com

Jennifer L. MacPherson
jmacpherson@bholaw.com

April 6, 2021

VIA CERTIFIED MAIL (RETURN RECEIPT)

RECEIPT NO. 7018 0040 0000 8022 5306

Brian Ternan, CEO
Health Net, LLC
Health Net of California, Inc.
Health Net Life Insurance Company
Health Net Community Solutions, Inc.
California Health & Wellness
21281 Burbank Blvd.
Woodland Hills, CA 91367

Re: *Vunisa v. Health Net, LLC, et al.*, Santa Clara Superior Court

Dear Mr. Ternan:

We represent Plaintiff, Joweli Vunisa ("Plaintiff"), and all other consumers similarly situated in a class action against Health Net, LLC, Health Net of California, Inc., Health Net Life Insurance Company, Health Net Community Solutions, Inc., California Health & Wellness, Centene Corporation (collectively, Health Net) and Accellion, Inc. (all together, "Defendants"), arising out of Defendants' failure to provide reasonable security for Plaintiff and the proposed class' personal information, which resulted in the unauthorized access and exfiltration, theft or disclosure of this information ("Data Breach"). To our knowledge, the Data Breach of Health Net members occurred on Accellion's legacy File Transfer Appliance (FTA) software from approximately January 7 to January 25, 2021 and was disclosed by Health Net on March 24, 2021 and publicly disclosed by Accellion in January 2021. Health Net was still using Accellion's 20 year old legacy FTA software despite known vulnerabilities, which put Health Net members' personal information at risk of this type of data breach.

The full claims, including the facts and circumstances surrounding these claims, are detailed in the Class Action Complaint, a copy of which is attached and incorporated by this reference.

Accellion's conduct constitutes violations of California Civil Code sections 1798.81.5(a)(1) and 1798.150(a)(1).

While the Complaint constitutes sufficient notice of the claims asserted, pursuant to California Civil Code section 1798.150(b)(1), Plaintiff demands that in the event a cure is possible, then within 30 days Health Net is hereby provided the opportunity to actually cure the noticed violation and provide Plaintiff with an express written statement that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and Plaintiff and the proposed Class members are not at risk of any of the information being used.

BLOOD HURST & O'REARDON | LLP

We await your response.

Sincerely,

JENNIFER L. MACPHERSON

JLM:jk

Enclosure

BLOOD HURST & O'REARDON | LLP

501 W. Broadway, Suite 1490 | San Diego, CA 92101
T | 619.338.1100 F | 619.338.1101
www.bholaw.com

Jennifer L. MacPherson
jmacpherson@bholaw.com

April 6, 2021

VIA CERTIFIED MAIL (RETURN RECEIPT)

RECEIPT NO. 7018 0040 0000 8022 5290

Michael F. Neidorff, CEO
Centene Corporation
7700 Forsyth Blvd.
St. Louis, MO 63105

Re: *Vunisa v. Health Net, LLC, et al.*, Santa Clara Superior Court

Dear Mr. Neidorff:

We represent Plaintiff, Joweli Vunisa ("Plaintiff"), and all other consumers similarly situated in a class action against Health Net, LLC, Health Net of California, Inc., Health Net Life Insurance Company, Health Net Community Solutions, Inc., California Health & Wellness, Centene Corporation (collectively, Health Net) and Accellion, Inc. (all together, "Defendants"), arising out of Defendants' failure to provide reasonable security for Plaintiff and the proposed class' personal information, which resulted in the unauthorized access and exfiltration, theft or disclosure of this information ("Data Breach"). To our knowledge, the Data Breach of Health Net members occurred on Accellion's legacy File Transfer Appliance (FTA) software from approximately January 7 to January 25, 2021 and was disclosed by Health Net on March 24, 2021 and publicly disclosed by Accellion in January 2021. Health Net was still using Accellion's 20 year old legacy FTA software despite known vulnerabilities, which put Health Net members' personal information at risk of this type of data breach. Centene Corporation is the parent of Health Net.

The full claims, including the facts and circumstances surrounding these claims, are detailed in the Class Action Complaint, a copy of which is attached and incorporated by this reference.

Accellion's conduct constitutes violations of California Civil Code sections 1798.81.5(a)(1) and 1798.150(a)(1).

While the Complaint constitutes sufficient notice of the claims asserted, pursuant to California Civil Code section 1798.150(b)(1), Plaintiff demands that in the event a cure is possible, then within 30 days Centene is hereby provided the opportunity to actually cure the noticed violation and provide Plaintiff with an express written statement that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and Plaintiff and the proposed Class members are not at risk of any of the information being used.

We await your response.

Sincerely,

JENNIFER L. MACPHERSON

JLM:jk
Enclosure

BLOOD HURST & O'REARDON | LLP

501 W. Broadway, Suite 1490 | San Diego, CA 92101
T | 619.338.1100 F | 619.338.1101
www.bholaw.com

Jennifer L. MacPherson
jmacpherson@bholaw.com

April 6, 2021

VIA CERTIFIED MAIL (RETURN RECEIPT)

RECEIPT NO. 7018 0040 0000 8022 5283

Jonathan Yaron, Chairman and CEO
Accellion USA, LLC
1804 Embarcadero Road, Suite 200
Palo Alto, CA 94303

Re: *Vunisa v. Health Net, LLC, et al.*, Santa Clara Superior Court

Dear Mr. Yaron:

We represent Plaintiff, Joweli Vunisa ("Plaintiff"), and all other consumers similarly situated in a class action against Health Net, LLC, Health Net of California, Inc., Health Net Life Insurance Company, Health Net Community Solutions, Inc., California Health & Wellness, Centene Corporation (collectively, Health Net) and Accellion, Inc. (all together, "Defendants"), arising out of Defendants' failure to provide reasonable security for Plaintiff and the proposed class' personal information, which resulted in the unauthorized access and exfiltration, theft or disclosure of this information ("Data Breach"). To our knowledge, the Data Breach of Health Net members occurred on Accellion's legacy File Transfer Appliance (FTA) software from approximately January 7 to January 25, 2021 and was disclosed by Health Net on March 24, 2021 and publicly disclosed by Accellion in January 2021.

The full claims, including the facts and circumstances surrounding these claims, are detailed in the Class Action Complaint, a copy of which is attached and incorporated by this reference.

Accellion's conduct constitutes violations of California Civil Code sections 1798.81.5(a)(1) and 1798.150(a)(1).

While the Complaint constitutes sufficient notice of the claims asserted, pursuant to California Civil Code section 1798.150(b)(1), Plaintiff demands that in the event a cure is possible, then within 30 days Accellion is hereby provided the opportunity to actually cure the noticed violation and provide Plaintiff with an express written statement that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and Plaintiff and the proposed Class members are not at risk of any of the information being used.

We await your response.

Sincerely,

JENNIFER L. MACPHERSON

JLM:jk

Enclosure